

OFFICE OF THE DIRECTOR

The Director is responsible to the Minister of Public Safety Canada (PS) for the control and management of the Service. He consults with the Deputy Minister of PS on the operational policy of CSIS, on applications for warrants and on any other matter for which the Minister indicates such consultation is needed. He also submits periodic reports about CSIS activities to the Minister, and chairs a number of internal committees which enhance the management and accountability of CSIS.

The Director is appointed for a period of up to five years by the Governor in Council. He may be eligible to be reappointed for one further term not exceeding five years.

DEPUTY DIRECTOR OPERATIONS (DDO)

Operations to collect information form the bedrock of intelligence, and it is under the auspices of the DDO that this central aspect of the Service's mandate is fulfilled. CSIS's primary collection discipline is human intelligence (HUMINT). The DDO is responsible for managing these efforts wherever they are undertaken, within an operating environment that is continually changing. The DDO's role is to support the Director on the overall management of the Service, which includes ensuring that the organization remains nimble, flexible and innovative while taking responsible risks in the delivery of our mandate and in the pursuit of strategic outcomes.

The DDO represents the Service and its strategic interests in a variety of forums within the domestic and international security and intelligence (S&I) community. Along with S&I partners, the DDO is involved in helping shape the Government of Canada's common front response to national security threats. The DDO is the Service Champion of our relationship with the Royal Canadian Mounted Police (RCMP) and the Canadian Association of Chiefs of Police (CACP).

The DDO Directorate is comprised of the following:

Assistant Director Collection (ADC): Manages and oversees all operational collection activity. The ADC is the Service Champion of our relationship with Global Affairs Canada (GAC) and National Defence (DND).

Assistant Director Operations (ADO): Responsible for the case management of all operational files at a national level along with our human sources. The ADO is the Service Champion of our relationship with Correctional Services Canada (CSC) and the National Parole Board (NPB).

Assistant Director Enablement (ADE): Responsible for the management of the Service's operational enablement functions, comprising of Scientific and Technical Services.

The ADE is the Service Champion of our relationship with the Communications Security Establishment (CSE), the Canada Revenue Agency (CRA) and the Financial Transaction and Reports Analysis Centre of Canada (FINTRAC).

DEPUTY DIRECTOR, ADMINISTRATION (DDA) AND CHIEF FINANCIAL OFFICER (CFO)

The DDA/CFO provides leadership on matters related to core business and infrastructure requirements, corporate governance and performance, and financial management.

The DDA/CFO directorate is comprised of the following Branches and Units:

- **Finance / Deputy Chief Financial Officer (DCFO):** Responsible for financial planning, budgeting and accounting, material management.
- **Chief Information Officer (CIO):** provides expert guidance on information management and technology related policies, planning and architectures
- **Strategic Management:** Provides advice, guidance and support to the Service in the areas of business planning, risk management and performance management.
- **Corporate Services (CS):** Manages, maintains, procures and disposes of real property and Service assets in response to corporate and directorate priorities.

ASSISTANT DIRECTOR, COLLECTION (ADC)

The ADC Directorate supports the Deputy Director, Operations (DDO) in the management and oversight of all operational collection activities

As a member of the Executive Team, the ADC represents the Service's Regional Offices and their strategic interests, primarily as it relates to their ability to efficiently and adequately accomplish their collection mandate.

The ADC is the Executive Champion of Service relationships with Global Affairs Canada (GAC) and the Department of National Defence (DND). The ADC is also the Executive Champion for Gender Equity.

The ADC Directorate is comprised of the following Regions:

- International Region (IR)
- Atlantic Region (AR)
- Quebec Region (QR)
- Ottawa Region (OR)
- Toronto Region (TR)
- Prairie Region (PR)
- British Columbia Region (BCR)

ASSISTANT DIRECTOR, HUMAN RESOURCES (ADH)

The Assistant Director, Human Resources is responsible for Human Resources Management (HRM) in the Service and is accountable to the CSIS Director on all HR matters. Its strategic outcome is to ensure the support, development and maintenance of a diverse, high-performing and sustainable workforce capable of meeting its mandate. The ADH is responsible for the strategic management of key areas including Learning and Development, Health and Workplace Management and Human Resources Services.

Directorate Mandate

- Provide policy and strategic advice to the Director and other Executive members on matters relating to human resources.
- Contribute to the development of the strategic vision of the Service and encourage ownership of human resources core principles and values.

- Develop innovative solutions to non-traditional problems, as well as short-term and long-term Management (HRM) strategies, including initiatives to make the organization a great place to work.
- Ensure HR initiatives are aligned with Public Service Renewal efforts and respond to internal and external corporate HR requirements
- Perform actively the elaboration of integrated business plans within the Service by ensuring HR priorities flow directly from business needs.
- Manage Executive compensation and Performance Management Agreements

Human Resources Core Principles

Valuing People:

At CSIS, employees are respected for their skills, their talents, and their contribution. One of the Service's priorities and one of the main responsibilities of supervisors and of managers is to help employees perform at their maximum. The principles outlined in this document apply to all employees, at all levels of the Service. Our actions and decisions will be aligned with these principles and everyone is respected and valued for their skills, talents and contributions.

- **People Matter:**
Honouring merit, mutual respect and equity
 - **Decision Making:**
Being consistent, fair, transparent, and accountable
 - **Communication:**
Engaging in open, clear and effective dialogue
 - **Diversity:**
Fostering inclusiveness and diversity of thought
 - **Learning:**
Encouraging lifelong personal development and professional growth
 - **Values:**
Demonstrating honesty, dedication, integrity and creativity
 - **Official Languages:**
Promoting and respecting the active use of both Official Languages.
 - **Work Environment:**
Providing a safe, secure, healthy, productive, and harassment/discrimination-free workplace
- The ADH Directorate is comprised of the following Branches and Section:
- Human Resources Services (HRS)
 - Learning and Development (LD)
 - Health and Workplace Management (HWM)

ASSISTANT DIRECTOR, LEGAL SERVICES (ADL)

In large corporations and in most government departments and agencies, the chief legal advisor is the General Counsel. The same is true at the Service, although the General Counsel is referred to as the Assistant Director, Legal (ADL). As the Service's chief legal advisor, the ADL heads a team of more than 100 lawyers and a support staff – that includes law clerks, legal analysts and administrative assistants – dedicated to providing a full range of advisory and litigation services in support of the Service's mandate.

Because of the delicate and sensitive work performed by a security intelligence agency, and the potential for infringement of legal rights of individuals and organizations, an intelligence agency must receive independent legal advice of the highest order and must follow that legal advice scrupulously. As a result, the office of the ADL is comprised of employees of the Department of Justice who do not come under the direction of Service managers. Working with the Service as a client, they are at all times accountable, through the ADL, to the Deputy Attorney General of Canada.

This allows legal staff the institutional independence they require to critically assess whether the Service's activities conform to Canadian law. It also allows them the institutional independence they require to provide the type of frank and impartial legal advice the Service must have if it is to perform its duties and functions in accordance with Canadian law and the expectations of Canadians.

Responsibilities:

- Support the Minister of Justice in working to ensure that Canada is a just and law-abiding society with an accessible, efficient and fair system of justice.
- Provide high-quality legal services and counsel to the government and to client departments and agencies.
- Promote respect for rights and freedoms, the law and the Constitution.

ASSISTANT DIRECTOR, OPERATIONS (ADO)

The ADO supports the Deputy Director, Operations (DDO) with the overall management of the Service's operational activities.

The ADO is responsible for an effective and accountable operations directorate with a forward-looking orientation. This is accomplished through a management framework that ensures effective, lawful, fiscally responsible, resource efficient, and policy-compliant operational activities that meet identified Government of Canada intelligence priorities.

The ADO represents the Service and its strategic interests in a variety of forums within the domestic and international security and intelligence (S&I) community, and helps shape the Government of Canada's response to national security threats.

The ADO Directorate is comprised of the following Branches:

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
" RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

HUMAN SOURCES AND OPERATIONS SECURITY

Provides support and advice on policy, source management and operational security to all Service Branches and Regions.

SECURITY SCREENING BRANCH (SSB):

The CSIS Security Screening program helps defend Canada and Canadians from threats to national security, including terrorism and extremism, espionage, and the proliferation of weapons of mass destruction. It is one of the most visible of the Service's operational sectors, primarily due to its dealings with government agencies and departments as well as members of the public, both domestic and foreign. Through its Government Security Screening and Immigration and Citizenship Screening programs, it helps the Government of Canada prevent persons who pose a threat to national security from obtaining access to classified or sensitive sites, government assets and information or major events, or from entering or obtaining status in Canada.

ASSISTANT DIRECTOR, POLICY AND STRATEGIC PARTNERSHIPS (ADP)

The Assistant Director, Policy and Strategic Partnerships (ADP) supports the Director and, through him, the Minister, in their accountability for the overall operational activities of the Service and provides strategic policy advice to the Director and Executive on areas falling under her purview.

Mandate

- Strengthen key partnerships, especially in the areas of strategic policy development and legislation.

- Advance Canadian government and Service interests.
- Solidify the Service's communication and reputation with key stakeholders and employees.
- Build qualitative and quantitative capacity in key areas of responsibility to ensure delivery of key objectives.

The ADP Directorate is comprised of the following Branches:

- **Communications Branch (CB):** Responsible for providing strategic communications advice, planning, production and evaluation in support of public and internal communications issues relating to the Service.
- **Emergency Management (EM) Branch:** Ensures the Service is in a constant state of operational preparedness and that its corporate and operational programs are continuously prepared to respond to, and recover from, an emergency or critical incident in a coordinated, timely and effective manner.
- **The External Review and Compliance (ERC) Branch:** Responsible for managing the Service's relationships with the Security Intelligence Review Committee (SIRC) and the National Security and Intelligence Committee of Parliamentarians (NSICOP). ERC is also the Service's policy centre for operational compliance.
- **Policy and Foreign Relations (PFR) Branch:** Responsible for coordinating and/or developing strategic-level policy within the Service, establishing and assessing the Service's foreign relationships;

ASSISTANT DIRECTOR, OPERATIONS ENABLEMENT (ADE)

The ADE Directorate supports the Deputy Director, Operations (DDO) with the management of the Service's operational enablement functions. The Directorate strives to enhance the overall operational effectiveness of the Service by providing innovative, timely and appropriate capabilities on pace with operational needs.

The ADE is the Service Champion of Service relationships with the Communications Security Establishment (CSE), the Canada Revenue Agency (CRA) and the Financial Transaction and Reports Analysis Centre of Canada (FINTRAC).

The ADE Directorate is comprised of the following Branches:

The **Scientific and Technical Services (STS)** Branch is responsible to advance Service operations through the provision of scientific and technical collection solutions

CHIEF INFORMATION OFFICER (CIO)

The CIO provides expert guidance on information management and technology related policies, planning and architectures. The CIO also represents the Service in the inter-departmental and international CIO community.

The CIO is responsible for the following Branches:

- **Information Management (IM) Branch:** IM provides information management services which facilitate the retrieval and availability of the right information to the right people at the right time.

CHIEF AUDIT AND EVALUATION EXECUTIVE

Mandate and Responsibilities

The Internal Audit and Evaluation Branch is made up of two sections: the Internal Audit and the Evaluation Sections. The Sections are led by a manager who reports to the Chief Audit and Evaluation Executive (CAEE). The CAEE reports directly to the Director and to the Departmental Audit Committee for internal audit activities and to the Performance Measurement and Evaluation Committee as Head of Evaluation.

The Internal Audit Section conducts engagements that provide management with an independent, objective assurance which is designed to add value and improve the Service's operations. It helps the Service accomplish its objectives by bringing a systematic, disciplined approach to assessing and improving the effectiveness of risk management, control and governance processes. Internal Audit aims to determine whether "we are doing things right."

The Evaluation Section conducts evaluations, reviews and consultations to provide management with neutral and credible information to inform decision-making, manage results and improve Service programs. Through a systematic and disciplined approach, the Evaluation Section examines the effectiveness and efficiency of key program areas in the Service. Evaluation aims to determine whether we "are achieving the results" and the extent to which the optimal amount of resources have been used.

Both Sections also work together to create an integrated risk-based annual plan, as well as through advisory/consulting engagements which require both skillsets. The approach in both Sections is comprehensive and collaborative. Program stakeholders are engaged throughout our processes and pertinent information is shared to ensure that the information is validated and value-added.

The CAEE is also the Senior Officer for Disclosure of Wrongdoing. The Senior Officer for Disclosure of Wrongdoing provides advice and assistance to employees who wish to report serious wrongdoing in the workplace and protects them against reprisal when they report wrongdoing in good faith.

SENIOR OFFICER FOR DISCLOSURE OF WRONGDOING

Mandate and Responsibilities

The Senior Officer for Disclosure of Wrongdoing provides advice and assistance to employees who wish to report serious wrongdoing in the workplace and protects them against reprisal when they report wrongdoing in good faith.

The CSIS Policy on Internal Disclosure of Wrongdoing and Reprisal Protection supports and strengthens the values that guide you - a CSIS employee - in your daily work and professional conduct. The policy encourages Service employees to come forward if they have reason to believe that serious wrongdoing has taken place. It provides protection against reprisal when employees do come forward, and ensures a fair and objective process for those against whom allegations are made.

Wrongdoing relates to serious violations that go against the public interest, such as:

- the violation of any federal or provincial law or related regulation;
- the misuse of public funds or public assets;
- gross mismanagement in CSIS or the federal public sector;
- a serious breach of CSIS Policy: Employee Conduct;
- doing something - or failing to do something - that endangers the life, health and safety of Canadians or the environment; or
- directing or counselling someone to commit a wrongdoing

The Senior Officer reports to the Director on all matters concerning internal disclosure of wrongdoing and reprisal protection and is responsible for the implementation and management of the policy. The Director has appointed the Chief Audit and Evaluation Executive to act as the Service's Senior Officer for Disclosure of Wrongdoing and has the overall responsibility for the CSIS Policy on Internal Disclosure of Wrongdoing and Reprisal Protection.

INTEGRATED TERRORISM ASSESSMENT CENTRE (ITAC)

Mandate and Responsibilities

The primary objective of the Integrated Terrorism Assessment Centre (ITAC) is to produce accurate, relevant and timely threat assessments on terrorism.

ITAC is a community-wide resource, housed within the CSIS national headquarters in Ottawa, and is in whole or in part, staffed by representatives from the following federal organizations: Public Safety Canada, the Canada Border Service Agency, Communications Security Establishment Canada, the Department of National Defence, the Department of Foreign Affairs and International Trade Canada, the Privy Council Office, Transport Canada, the Correctional Service of Canada, the Financial Transactions and Reports Analysis Centre of Canada, Public Works and Government Services Canada, the Royal Canadian Mounted Police, the Canada Revenue Agency and the Canadian Security Intelligence Service. These representatives bring the information and expertise of their respective organizations to ITAC.

The National Security Advisor (NSA), in consultation with the Director of CSIS, is responsible for appointing the Executive Director of ITAC for a two-year term. The ITAC Executive Director meets each year with the National Security Advisor and deputy ministers from each key partner organization. The purpose of these meetings is to review ITAC's performance; provide guidance on the focus, effectiveness, and efficiency of ITAC activities; and

strategically orient threat assessment priorities. As a component of CSIS, ATAC is subject to review by the Security Intelligence Review Committee (SIRC) and the office of the Inspector General (IG).

ACADEMIC OUTREACH (AO)

Mandate and Responsibilities

AO provides the Service with a better understanding of current and emerging security issues by drawing regularly on knowledge from experts in a variety of disciplines. The goal is to develop a long-term view of various trends and problems, to challenge our own assumptions and cultural bias, as well as to sharpen our research and analytical capacities.

Responsibilities:

- Design, plan and/or host several activities, including conferences, seminars, papers, presentations and round-table discussions.
- Provide essential contextual knowledge in support of Service collection and assessment capacity.
- Build partnerships with government stakeholders in support of an integrated threat assessment capability.
- Promote academic research on security issues useful to the making of public policy and the emergence of a more informed public debate on security.

COMMUNICATIONS BRANCH (CB)

Mandate and Responsibilities

CB's role is to explain to Canadians the Service's mandate and contribution to national security and to help managers communicate the objectives of the Service to employees. CB is responsible for the overall planning, management and evaluation of both internal and external communication. CB works closely with other government counterparts, such as Public Safety, the Privy Council Office and the Minister's office and ensures corporate communications plans and strategies support broader corporate objectives and Government of Canada communications policies.

CB's responsibilities include:

- Identifying corporate communications needs;
- Advising senior management;
- Developing internal and external communications strategies;
- Communicating in a timely manner (in both official languages) with the public and the media;
- Providing advice and support to program managers for multimedia services;
- Ensuring the Service has the communications products it needs to communicate with partners and stakeholders;
- Cooperating with other departments and agencies to ensure effective and coherent communications with the media and the public.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

Canada's national security continues to be threatened by espionage, foreign influenced activity and terrorism.
in accordance with sections 2(a)(b)(c) of the CSIS Act, is
responsible for investigating acts of:

- (a) **espionage or sabotage** against Canada that is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage
- (b) **foreign influenced activities** within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person
- (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

CORPORATE SERVICES (CS)

Corporate Services Mandate

We move CSIS forward. We ensure that all employees have a safe, healthy, secure and fit-for purpose work space, including the additional goods and services needed to support all CSIS programs. We ensure that other critical services are in place to facilitate this goal from cleaning, contractor clearances, maintenance, mail services, shipping/receiving, asset management, space management and print shop. We provide other essential work tools such as the conference centre, theatre, furniture, parking and stores. We plan and execute major capital projects that keep work-space responsive to the needs of CSIS. We look ahead to support innovation and to ensure that all resources dedicated to this effort are utilized in a manner that delivers best value to the Crown. We ensure the application of relevant legislation, regulation and government policy

applicable to Real Property, Procurement and Asset Management. We work closely with internal and external stakeholders to ensure that we can achieve this vision.

CS is always looking to create opportunities for motivated employees with interests and qualifications in project management, procurement, logistics, administrative support, contract clearance support, space management, and print shop specialists.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
" RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION "

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
" RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION "

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
" RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION "

EXTERNAL REVIEW AND COMPLIANCE (ERC)

Mandate and Responsibilities

The role of CSIS in protecting Canada's national security interests is a vital one. While the work we do is clandestine in nature, it is not without public accountability. The CSIS Act not only equips the Service with intrusive powers to conduct our operations, but also provides for robust external review mechanisms.

The External Review and Compliance (ERC) Branch is responsible for managing the Service's relationships with the Security Intelligence Review Committee (SIRC) and the National Security and Intelligence Committee of Parliamentarians (NSICOP). ERC is also the Service's policy centre for operational compliance. ERC is comprised of three units: Review, Complaints, and Compliance.

FINANCE BRANCH

Mandate and Responsibilities

The Finance Branch manages the Service's core finance functions such as budgeting, accounting, resource and planning, and financial reporting.

Finance supports the mandate of Deputy Director, Administration and Chief Financial Officer by providing assistance in the following areas:

- Advising on business and financial management.
- Stewardship with respect to relevant legislation, regulations, policies, directive and standards related to financial management.
- Program financing, financial/administrative reporting and disclosure, and dealing with central agencies.

HUMAN RESOURCES SERVICES (HRS)

Mandate and Responsibilities

HRS is responsible to oversee a consistent, cohesive, coherent and integrated approach to human resources management. This includes the development, administration and implementation of human resources policies and practices, as well as providing advice to management and employees on human resources/compensation matters.

HUMAN SOURCES AND OPERATIONS SECURITY (HSOS)

Mandate and Responsibilities

Provides support and advice on policy, source management and operational security to all Service Branches and Regions.

HEALTH AND WORKPLACE MANAGEMENT (HWM)

Mandate and Responsibilities

Health and Workplace Management (HWM) branch is comprised of a number of programs that contribute to the achievement of a diverse, high performing and sustainable workforce while ensuring a safe, healthy and respectful work environment.

HWM branch is responsible for:

- Health and Wellness
 - Psychological Health and Safety
 - Occupational Health and Safety
 - National Wellness Coordinator
 - Internal Conflict Management Services (ICMS)
- Workforce Analytics
- Human Resources Systems
- Official Languages
- Translation Services
- Diversity
- Values and Ethics
- Labour Relations

INTELLIGENCE ASSESSMENTS BRANCH (IAB)

Mandate and Responsibilities

IAB's mandate is to provide timely and relevant intelligence which meets the Government of Canada's (GoC) stated requirements and priorities. Within the Service, IAB is responsible for prioritizing and integrating intelligence requirements from all sources and for providing subject-matter expertise in support of collection, reporting and Executive briefing needs.

IAB's responsibilities include:

- Actively engage with the GoC to identify its intelligence needs and deliver briefings, assessments and reports which meet the strategic requirements of GoC senior policy-makers.
- Work closely with other operational Branches to prioritize and integrate intelligence requirements from all sources.
- Provide subject-matter expertise in support of operational and administrative programs.

- Maintain open-source information services tailored to meet the operational and corporate requirements of the Service.

- Provide outreach and education to GoC consumers.

INTERNAL CONFLICT MANAGEMENT SERVICES (ICMS)

Internal Conflict Management Services' (ICMS) mandate is to deliver training and interventions to support the prevention, management and resolution of workplace conflict in a way that promotes a respectful, healthy and productive environment that contributes to operational effectiveness.

ICMS offer informal interest-based conflict resolution methods (such as conflict coaching, facilitated discussions, mediation and group processes), as well as conflict management training.

ICMS practitioners help managers, supervisors, and non-supervisory staff resolve workplace conflict promptly and constructively by providing informal and collaborative conflict resolution approaches and courses. These methods allow parties to move from a formal process (grievance or harassment complaint) to an informal process, while maintaining their right to return to the formal process should they wish if an agreement cannot be reached. (Section 4.4 – Resolution of Harassment Complaints)

The ICMS Program has three main pillars:

Impartial: ICMS is a third-party impartial body that objectively supports all managers and employees in determining the most appropriate option to resolve their conflict situation. To maintain impartiality, ICMS practitioners do not represent employees nor do they advocate on their behalf.

Confidential: Consultations and services provided by ICMS are always kept confidential with the exceptions of the following:

- The information provided by the individual suggests a threat to human life and safety;
- Access to Information Act and the Privacy Act legislation;
- As required by law or judicial authority;
- Where obligations arising from terms of settlement necessitate the involvement of a third client; and
- ICMS have been authorized in writing by the clients to share the information with others.

All parties, including anyone who accompanies a client in an ICMS meeting or process, are expected to keep any information gained during that process confidential.

Voluntary: ICMS services are voluntary. Employees at all levels (including managers) should be informed by their supervisor of our services as an option to resolve conflict as soon as possible to prevent the situation from escalating further.

INFORMATION MANAGEMENT (IM)

Mandate and Responsibilities

IM provides information management services which facilitate the retrieval and availability of the right information to the right people at the right time.

the Branch provides an effective information management program to foster informed decision making and preserve and ensure access to information and records for the benefit of the Service as a whole.

IM is responsible for:

- Managing corporate information throughout its lifecycle,
- Supporting clients in the retrieval of information
- Leading initiatives/projects that have service-wide benefits;
- Managing client services relating to information/system access
- Providing IM Liaison services to assist clients in understanding how to manage their information and to raise awareness of their responsibilities related to information management;
- Providing Strategic Planning, Policy and Oversight services to meet IM accountability requirements, coordinate responses to internal/external audits, and perform policy reviews and compliance;
- Ensuring that the Service's business requirements are aligned strategically with IM architecture and requirements.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

INTERNAL SECURITY (IS)

Mandate and Responsibilities

Internal Security is responsible for managing the development and implementation of the national security program to protect CSIS, its assets, operations and employees from all security threats.

The three principle sectors in Internal Security, and their areas of responsibilities, are as follows:

Personnel Security

Responsibilities include:

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

Infrastructure Security

Responsibilities include:

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

Management Services

Responsibilities include:

LEARNING AND DEVELOPMENT (L&D)

Mandate and Responsibilities

The Learning and Development Branch (L&D) ensures that Service managers and employees have the right skills, knowledge and abilities to fulfill the organizational mandate and deliver on strategic priorities. Building a culture where continuous learning is an organizational "way of life" that is encouraged, supported and rewarded as a necessary business practice that assists in employee development, management and engagement is our long term goal.

L&D program responsibilities consist of the following core objectives:

- Provide the knowledge, skills and competencies all employees require to perform their duties effectively.
- Support the growth and development of Service employees throughout their careers.
- Provide the skills, awareness, and knowledge necessary to protect our employees in the performance of their duties.
- Cultivate management excellence, promote organizational rigour, and enhance leadership capacity.
- Support the evolution of intelligence gathering methodology and operational doctrine.
- Enable specialists in specific functional categories to meet and maintain their professional standards.

LITIGATION AND DISCLOSURE BRANCH

Mandate and Responsibilities

Litigation and Disclosure Branch coordinates and supports the disclosure of Service information/intelligence as part of domestic and foreign judicial proceedings, and ensures its protection via the national security provisions in the Canada Evidence Act. The Branch also works closely with operational branches, regional offices, relevant policy centres, Legal Services and the Department of Justice.

The onslaught of litigation is presenting serious challenges to the protection of ongoing investigations and Service methodology. It is only through the rigorous management of disclosure that the Service can continue to meet both the requirements of its statutory mandate, and the priority in maintaining and building upon its relationships/partnerships.

Responsibilities include:

- Provide assistance in the preparation of disclosure strategies
- Cross-reference cases for consistency
- Build expertise for witness/affiant preparation

- Provide strategic advice to Executive and Service personnel on disclosure
- Provide regular updates to Executive of significant litigation issues.

MATERIEL MANAGEMENT AND ACQUISITIONS (MMA)

Mandate and Responsibilities

Materiel Management and Acquisitions (MMA) is responsible for core administrative functions surrounding acquisitions, asset management, shipping and receiving, mail/courier services,

MMA supports the Assistant Director, Finance and Administration / Deputy Chief Financial Officer by providing:

- Advice on warehousing/storage, (including mail).

POLICY AND FOREIGN RELATIONS

Strategic Policy coordinates and/or develops most strategic level policy issues within the Service.

Foreign Relations is responsible for the establishment, coordination and ongoing assessment of the status of the Service's foreign relationships.

The Policy Section administers the CSIS System which is comprised of several essential Service documents, including the Service's policy documents

Management Services fulfills all administrative and corporate requirements for the Branch

STRATEGIC POLICY

Mandate and Responsibilities

The Strategic Policy is responsible for the coordination and/or development of most strategic-level policy issues within the Service. The unit ensures that the Executive is kept informed of broader government initiatives and direction, and that the interests of and advice from the Service are properly represented at the strategic level, including the Privy Council Office, the National Security Advisor, and the Minister of Public Safety.

In fulfilling its functions, Strategic Policy is tasked with:

- **Cabinet:** Maintaining an awareness of and appropriate level of involvement in Cabinet business, and sharing updates and developments with branches of the Service and the Executive.

- **Parliament:** Tracking the work of Parliament for issues of interest to the Service and, when required, preparing government responses to committee reports, speeches for Parliamentary debates and briefing materials for officials
- **PCO and Minister's Office:** Acting as a point of contact for the Privy Council Office and the Minister's office, related to requests for information, security verifications and Inquiries of Ministry
- **Briefing Notes:** Preparing all formal Briefing Notes destined for external, senior government audiences, most notably the Minister and/or the National Security Advisor.
- **Correspondence:** Researching and preparing responses to correspondence on behalf of the Director and Minister.
- **Strategic Planning and Partnerships:** Coordination and production of Corporate Priorities and management of Domestic Liaison Program.
- **Briefing support for Director:** Coordination and preparation of briefing material in advance of Director's participation at DM committees and bilateral meetings, as well as drafting of some decks and speaking points for the Director's use.
- **Strategic Policy - General:** Various ad hoc tasks, including coordination of briefing material for transition of Minister and Director, production of Strategic Insight, support to Strategic Review etc.

FOREIGN RELATIONS

Mandate and Responsibilities

FR is responsible for the establishment, coordination, and ongoing assessment of the Service's foreign relationships. Through collaboration with external partners – including Public Safety Canada (PS) and Global Affairs Canada (GAC) – as well as CSIS operational and corporate branches, FR manages and oversees corporate foreign relations matters.

In fulfilling its functions, FR is tasked with:

- **Section 17(1)(b) Foreign Arrangements:** Coordination of corporate requirements linked to the implementation of new, or enhancements to existing, CSIS foreign arrangements.
- **Liaison:** Management of the Service's relationships with Foreign Liaison Representatives (FLRs)

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
"RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION"

- **Briefing Material:** Drafting of briefing material for members of the Executive Committee. This includes tasking branches for input, editing material provided, and ensuring relevancy, accuracy, and timeliness.
- **Courtesy Letters:** Researching and preparing responses to courtesy letters received from foreign agencies addressed to the CSIS Director and DDO (i.e. farewell, congratulatory, condolence; invitations).
- **Security Intelligence Review Committee Requirements:** Researching and preparing responses to Security Intelligence Review Committee (SIRC) requests related to the implementation and corporate management of CSIS foreign arrangements.

- **International Policy:** Coordination of Service engagement with Canadian departments and agencies on national security issues that have an international affairs nexus.
- **Foreign Relations – General:** Various ad hoc tasks, including the coordination of events, production of statistics and weekly updates, support to partner agencies, provision of protocol-related advice, promotion of s.17(1)(b) foreign requirements.

POLICY SECTION

Mandate and Responsibilities

CSIS System

The Policy Section is responsible for administering the CSIS System which is comprised of several essential Service documents, including the Service's policy documents

The Policy Section ensures that policy documents are consistent with the CSIS Policy Framework. Policy documents must also adhere to Ministerial Direction, Treasury Board Policies, the CSIS Act and other legislation.

As well, the Policy Section provides employees and Policy Centres with guidance and support regarding the as well as assists with, or provide context to, historical information on Service policies, procedures and domestic arrangements.

Developing CSIS Policies and Procedures

The Policy Section is responsible for developing new policies and procedures and evaluating existing policy documents. This process involves analyzing, in conjunction with the Policy Centre, all existing policy documents to determine where they fit within the policy model. Based on the results of the analysis, the Policy Section may recommend the transfer of guidance and information documents to the Policy Centre's webpage or develop new policy documents using the policy model standards.

When policies and procedures are created, the Policy Section may conduct limited, Service-wide consultations to ensure that the policy documents are clear and effective.

Coordinating the Development of Domestic Arrangements

The Policy Section, in conjunction with the Policy Centre, coordinates the development, review, and approval process of domestic arrangements pursuant to s.17(1)(a) of the CSIS Act between the Service and a department of the Government of Canada or another party.

The Policy Section also coordinates the Ministerial and Executive approval process of s.13(2)(a) and (b) of the CSIS Act arrangements (Security Assessments).

Maintaining the CSIS

System

The Policy Section is responsible for maintaining various Service documents. These documents include the Policy Framework, Corporate Ministerial Direction, CSIS Strategic Plan and Priorities, Collective Agreement as well as Acts and Legislation.

The Policy Section is also responsible for the following:

- Efficient and effective research and analysis of policies and procedures with the objective of eliminating confusion and contradictions;
- The development of professional expertise, corporate memory and best practices in the development and publication of policies and procedures;
- Managing and coordinating the policy review, development, and approval process to ensure consistency with relevant ministerial direction, legislation, Treasury Board Policies and other government standards;
- Standardizing the terms and references used throughout Service policies and procedures

Policy and Foreign Relations - Management Services

Management Services Unit coordinates the PFR Branch responses to corporate requirements

The unit is also responsible for the production of responses to requests for Access to Information and Privacy (ATIP), Security Intelligence Review Committee (SIRC) and National Program Overview (NPO's) on behalf of the Branch.

The unit ensures the proper coordination of financial and human resources. It manages PFR's accommodations, procurement, informatics, and training and development requirements with proper planning and/or follow-up of related activities, initiatives and submissions.

Management Services works closely with the various policy centers such as Recruitment and Staffing, Information Management, Learning and Development as well as Official Languages to ensure the OLIF is completed for every position and reviewed at every staffing action. It provides advice to management on the development of position profiles, objectives and Performance Evaluation Reports (PER's).

The unit maintains an organized list of positions with incumbent information and updates the Branch Organizational Chart. It liaises with the Awards Coordinator for nomination of Branch employees to the Employee Recognition and Awards Program.

STRATEGIC MANAGEMENT (SMB)

Mandate and Responsibilities

The Strategic Management Branch (SMB) is the centre of expertise for integrated planning, risk, performance management, investment governance and investment planning within the Service.

Effective planning and management towards results is fundamental to the success of any government department or agency. SMB provides guidance and support to the Executive, Directorates and managers in the business planning, risk and performance management activities within the Service. The branch is responsible for ensuring the principles of sound planning, strategic priority setting, risk identification, monitoring of performance and management towards results are integrated into the management of Service programs and branches. This facilitates sound decision-making and overall successful program delivery. In addition, SMB is responsible for creating a more structured approach for investment planning and decision-making to govern the Service's investments. This provides clarity on where we are investing our resources and where we need to invest next.

Our vision

Service managers have the tools, knowledge and support required to effectively plan, prioritize, manage and monitor their programs. Service managers consider risk and performance information to make sound decisions and effectively deliver programs to achieve results.

SMB carries out its mandate through the following activities:

- Direction, guidance and oversight of the integrated planning, monitoring and reporting cycle
- Policy centre for strategic planning, business planning and investment planning
- Policy centre for risk and performance management
- Provision of corporate framework, guidance tools, training, advice and facilitation for business planning, investment governance, risk management and performance management and reporting
- Facilitate the development of corporate strategic direction and documents
- Management of CSIS stewardship with respect to Government of Canada policy related to management accountability, results and performance (MAF, PoR Risk Management, Investment Planning)

SECURITY SCREENING BRANCH (SSB)

Mandate and Responsibilities

Often referred to as Canada's "first line of defence", CSIS Security Screening Branch (SSB) is an important, primary means of keeping Canada and Canadians safe from threats to national security.

Of the two major operational programs mandated by the CSIS Act, the Security Screening program is perhaps the most visible across government, providing threat-related security assessments or advice to Government of Canada (GoC) clients.

Acting under the authority of ss. 13, 14 and 15 of the CSIS Act, SSB operations:

- prevent persons of national security concern from gaining access to classified or sensitive government information, assets, sites or major events; and
- help prevent non-Canadians who pose a threat to national security from entering or acquiring status in Canada.

Through its two sub-programs – Government Security Screening (GSS) and Immigration and Citizenship Screening (ICS) – SSB investigates, analyses and provides assessments or advice on a wide range of national security threats, including terrorism and extremism, as well as espionage, foreign interference and the proliferation of weapons of mass destruction.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
"RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION"

SCIENTIFIC AND TECHNICAL SERVICES (STS)

Mandate and Responsibilities

STS provides scientific and technical collection solutions and knowledge

We accomplish this through the highest quality personnel, technology and practices.

ATLANTIC REGION (AR)

Mandate and Responsibilities

AR is responsible for
Island, and Newfoundland and Labrador.

the provinces of Nova Scotia, New Brunswick, Prince Edward

BRITISH COLUMBIA REGION (BCR)

Mandate and Responsibilities

BCR is responsible for fulfilling the Service's mandate in the province of British Columbia (B.C.) and Yukon Territory, and conducts regional investigations by collecting, analyzing, and reporting intelligence.

The head office of BCR is located in

Burnaby, B.C.

INTERNATIONAL REGION (IR)

Mandate and Responsibilities

International Region (IR) is responsible for carrying out the Service's mandate abroad.

OTTAWA REGION (OR)

Mandate and Responsibilities

OR, co-located with HQ, is responsible for fulfilling the Service's mandate

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

PRAIRIE REGION (PR)

Mandate and Responsibilities

PR is responsible for the execution of the Service's mandate in the provinces of Alberta, Saskatchewan,
Manitoba
Edmonton, Alberta.

The Region is comprised of a Regional headquarters located in

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

QUEBEC REGION (QR)

Mandate and Responsibilities

QR is responsible for carrying out CSIS's mandate in most of the province of Quebec.

QR has a regional office in Montreal.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

TORONTO REGION (TR)

Mandate and Responsibilities

TR headquarters is located

in downtown Toronto.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

EMPLOYEES' ASSOCIATION

Mandate and Responsibilities

The Employees' Association (EA) is responsible for providing support to all non-unionized employees in dealing with the senior management of the Service. In addition, the Association fosters co-operative initiatives on matters pertaining to the policies/programs of the Service and its membership. The Association believes in a two way commitment to ensure the well-being of its members and the fulfilment of the Service's mandate. The EA's objectives are to:

- Bring to the attention of CSIS management problems and concerns of employees through the established Employee/Employer Consultation (EEC) process.
- Consult senior management in the resolution of employee concerns via oral and/or written submissions.
- Support Service policies and programs upon completion of the consultative process.
- Represent employees in the resolution of their complaints and grievances, including the application of Human Resources policies, and provide assistance to employees facing disciplinary action.

To help meet these objectives, Employees' Association is made-up of three members: the President and two Officers. Regional and headquarter representatives are elected by Association members in each Region and Headquarters to serve on the Association Executive Council.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
« RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION »

ASSISTANT DIRECTOR, INTELLIGENCE (ADI)

The ADI reports to the Director of CSIS on all intelligence assessment and production matters and is responsible for all aspects of information dissemination. This process enhances the government's awareness of the nature and magnitude of threats; assists decision makers in efforts to counter these threats; supports the mandates of other domestic and foreign partners, and identifies gaps and emerging issues regarding the national security agenda.

Furthermore, the ADI represents the Service in a variety of organizational and strategic interests. These include directional responsibilities which contribute to the Canadian intelligence assessment community. As an Assistant Deputy Minister responsible for intelligence, the ADI is also a principal representative for special briefings and engagements at committees, forums and seminars.

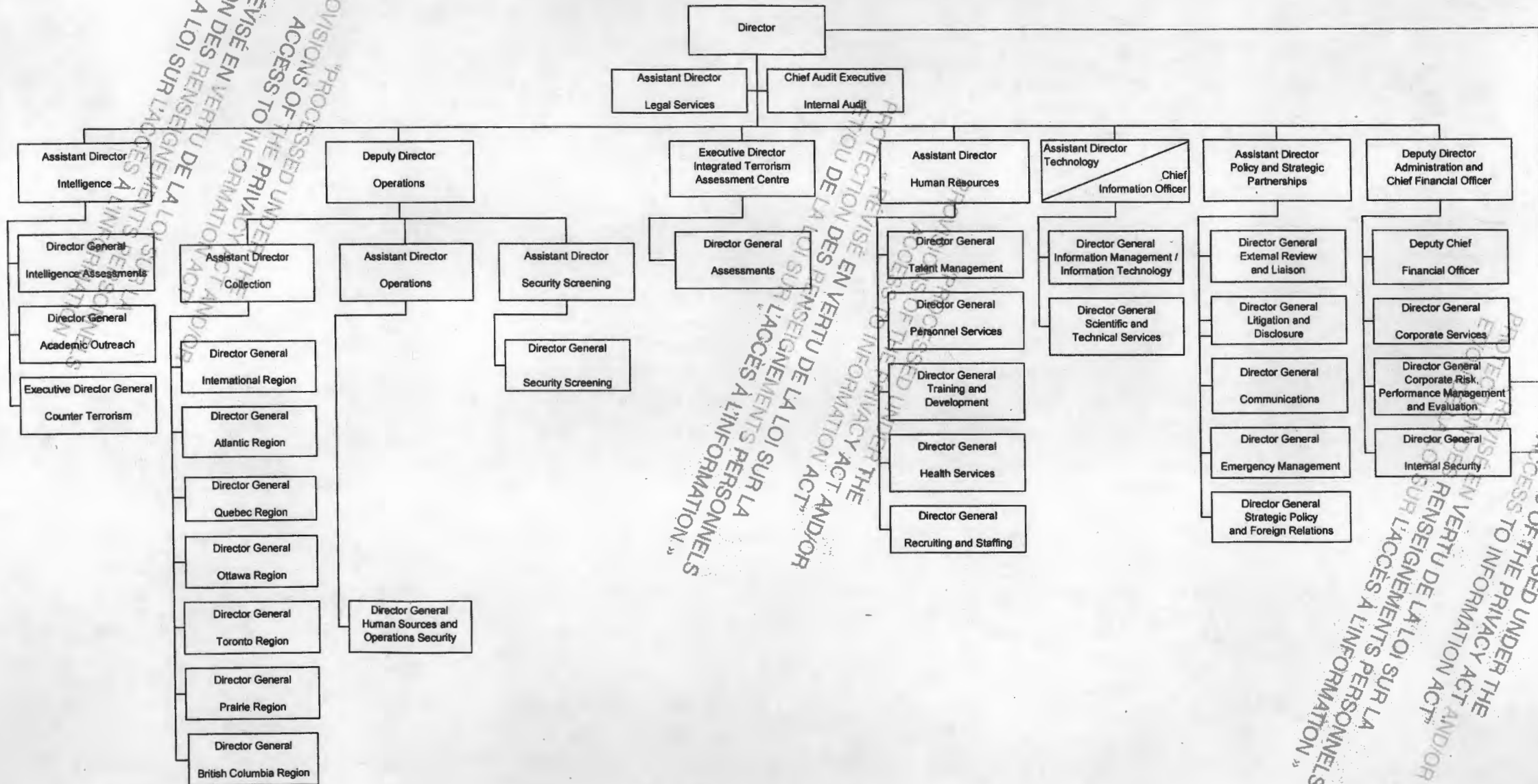
The ADI Directorate is comprised the following Branches:

- **Litigation and Disclosure Branch:** Coordinates the disclosure of Service information during domestic and foreign judicial proceedings (civil, criminal and administrative) and works closely with operational branches, regional offices, relevant policy centers, Legal Services and the Department of Justice.
- **Intelligence Assessments:** Provides timely and focussed intelligence, prioritizing in support of collection and reporting.
- **Academic Outreach:** Draws on the knowledge of experts from a variety of discipline so the Service can foster a contextual understanding of security issues.

The ADI is also a conduit for the Service's interaction with the Integrated Terrorism Assessment Centre (ITAC), which is responsible for producing integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities, first-line responders such as law enforcement, and as appropriate, critical infrastructure stakeholders in the private sector.

"PROCESSED UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT"
"RÉVISÉ EN VERTU DE LA LOI SUR LA
PROTECTION DES RENSEIGNEMENTS PERSONNELS
ET/OU DE LA LOI SUR L'ACCÈS À L'INFORMATION"

CANADIAN SECURITY INTELLIGENCE SERVICE



2013-07-13
Date

[Signature]
Interim Director